Close interaction, incompatible regimes, contentious challenges: the transnational movement to protect privacy

Tarrow, Sidney

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Wissenschaftszentrum Berlin für Sozialforschung (WZB)

Tarrow, Sidney

Working Paper

Close interaction, incompatible regimes, contentious challenges: The transnational movement to protect privacy

WZB Discussion Paper, No. SP IV 2017-102

Provided in Cooperation with:
WZB Berlin Social Science Center

Suggested Citation: Tarrow, Sidney (2017) : Close interaction, incompatible regimes, contentious challenges: The transnational movement to protect privacy, WZB Discussion Paper, No. SP IV 2017-102, Wissenschaftszentrum Berlin für Sozialforschung (WZB), Berlin

This Version is available at:
http://hdl.handle.net/10419/156334

WZB
Berlin Social Science Center

Sidney Tarrow

CLOSE INTERACTION, INCOMPATIBLE REGIMES, CONTENTIOUS CHALLENGES:
The Transnational Movement to Protect Privacy

Discussion Paper
SP IV 2017–102
February 2017

WZB Berlin Social Science Center
Research Area
International Politics and Law
Research Unit
Global Governance

Wissenschaftszentrum Berlin für Sozialforschung gGmbH
Reichpietschufer 50
10785 Berlin
Germany
www.wzb.eu

Sidney Tarrow
sgt2@cornell.edu

CLOSE INTERACTION, INCOMPATIBLE REGIMES, CONTENTIOUS CHALLENGES:
The Transnational Movement to Protect Privacy
Discussion Paper SP IV 2017–102
Wissenschaftszentrum Berlin für Sozialforschung (2017)

Affiliation of the authors other than WZB

Sidney Tarrow
Cornell University

Abstract

CLOSE INTERACTION, INCOMPATIBLE REGIMES, CONTENTIOUS CHALLENGES:
The Transnational Movement to Protect Privacy[1]

by Sidney Tarrow

Scholars and legal practitioners have found profound differences between the privacy practices of Europe and the United States. This has produced incompatible regimes of regulation, causing serious normative and political issues. This conflict – originally centered on the exchange of commercial data -- became increasingly more acute after 9/11, as American policy-makers saw digital data as a major source of intelligence and Europeans become frightened of the impact of American surveillance. On the cusp of 9/11, the EU and the US had negotiated a peculiar mixed-level agreement – the "Safe Harbor" agreement -- to regulate the behavior of firms exchanging data across the Atlantic. The Snowden affair and related revelations showed how badly this agreement worked, producing incentives for European advocates to challenge "Safe Harbor" in court in 2015, resulting in a new – but still untested – agreement in 2016, and influencing the shape of the EU's new data regulatory authority.

These interactions raise three kinds of problems for scholars of global governance and social movements: First, how does the combination of close interaction and incompatible regimes affect the capacity of states and other actors to resolve problems of international collaboration? Second, how have international institutions responded to these challenges? Third, such disputes raise the puzzle of how digital globalization has affected the difficult process of the formation of transnational movements. I will argue that – two decades after the start of digital globalization – it has taken critical junctures like 9/11 and the Snowden revelations to produce the political opportunity for the formation of a trans-Atlantic movement on behalf of privacy.

Keywords: privacy, transatlantic movements, safe harbor, privacy shield

---

[1] This paper is a revised version of a colloquium paper presented to the Global Governance Department at the Berlin Social Science Center in October, 2016. I wish to record my gratitude to Henry Farrell, Abe Newman, Pris Regan, Christian Kreuder-Sonnen, and Lee Tien for their help in the preparation of this paper and to Emilio Lehoucq for the research assistance for the empirical analysis in Part Five. I would also like to thank Colin Bennett, Lance Bennett, Mike Dorf, Kristin Eichensehr, Christian Kreuder-Sonnen, Gary Marks, Jörg Pohle, Agustin Rossi. Rebecca Slayton, Ben Wagner and the members of the Internet Policy Group at the WZB for comments on a draft of the paper. The title, as well as the organization of the material, was suggested by Bob Keohane, adding to three decades of collegiality and friendship.

Zusammenfassung

ENGE WECHSELWIRKUNGEN, INKOMPATIBLE REGIME, UMSTRITTENE HERAUSFORDERUNGEN
Die transnationale Bewegung zum Schutze der Privatsphäre

von Sidney Tarrow

Wissenschaftler und Rechtsanwälte haben tiefgreifende Unterschiede zwischen den Datenschutzpraktiken Europas und den Vereinigten Staaten gefunden. Dies hat zu unvereinbaren Regulierungsregimen geführt, welche ernsthafte normative und politische Probleme darstellen. Dieser Konflikt, der sich ursprünglich auf den Austausch von kommerziellen Daten konzentrierte, wurde nach dem 11. September zunehmend akuter, da die amerikanischen Entscheidungsträger die digitalen Daten als wichtige Intelligenzquelle sahen und die Europäer Angst vor den Auswirkungen der amerikanischen Überwachung entwickelten. Im Kontext des 11. September hatten die EU und die USA eine Vereinbarung - das "Safe Harbor" - Abkommen ausgehandelt, um das Verhalten von Firmen zu regeln, die Daten über den Atlantik austauschen. Die Snowden-Affäre und die damit zusammenhängenden Enthüllungen zeigten jedoch, wie schwach diese Vereinbarung war. So konnten Anreize für die europäischen Befürworter geschaffen werden, um "Safe Harbor" im Jahr 2015 vor Gericht anzufechten. Dies führte demzufolge im Jahr 2016 zu einer, noch nicht getesteten, Vereinbarung, welche die Form der neuen EU-Regulierungsbehörde beeinflussen könnte. was zu einer neuen - aber noch nicht getesteten - Vereinbarung im Jahr 2016 führte und die Form der neuen EU Datenregulierungsbehörde beeinflusst.

Diese Wechselwirkungen werfen drei grundsätzliche Probleme für Wissenschaftler der Global Governance und sozialer Bewegungen auf: Erstens, beeinflussen die Kombination von enger Interaktion und inkompatiblen Regimen die Fähigkeit von Staaten und anderen Akteuren, Probleme internationaler Zusammenarbeit zu lösen? Zweitens, wie haben internationale Institutionen auf diese Herausforderungen reagiert? Drittens, stellen solche Auseinandersetzungen dar, wie die digitale Globalisierung den schwierigen Prozess der Bildung transnationaler Bewegungen beeinflusst hat? Ich behaupte, dass es - zwei Jahrzehnte nach Beginn der digitalen Globalisierung - kritische Umstände wie den 11. September und die Snowden-Enthüllungen brauchte, um die politische Chance zur Bildung einer transatlantischen Bewegung im Namen der Privatsphäre zu schaffen.

Stichwörter: Datenschutz, transatlantische Bewegung, safe harbor, privacy shield

This paper is dedicated to the memory of Alan Westin, who encouraged me to publish my first article, which emerged from a term paper written for his course at Columbia in 1961.

On October 5, 2015, The Court of Justice of the European Union (CJEU) ruled that the United States' "Safe Harbor" agreement, which has, since 2000, regulated the transfer of data of European origin to the United States, was invalid.[2] The ruling came when an Austrian privacy advocate, Max Schrems, brought a case to the Court against Facebook, which maintains its European data center in Ireland. Schrems claimed that his privacy had been violated by the U.S. National Security Agency's mass-surveillance programs, which had been revealed by whistle-blower Edward Snowden in 2013 to be sweeping up enormous amounts of data – some of it European in origin[3]. The Irish data protection agency held that it had no authority to monitor what Facebook did with the data it transferred from Europe to the U.S.[4] and the Irish High Court referred the dispute to the CJEU, which decided that the Safe Harbor agreement was incompatible with EU laws and conventions.[5]

What is Happening Here?

This story illustrates three things that will guide the analysis that follows:

First, firms like Facebook and their ability to move data quickly across borders constitute the "close interaction" in the first part of the title of this paper.

---

[2] The Safe Harbor documents can be found at http://www.export.gov/safeharbor and in European Union Data Protection Working Party 2001, *Opinion 1/2001 on the Draft commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46, 5102/00/EN WP 38*. The nuts and bolts of the agreement are briefly described by Colin Bennett and Charles Raab in their primer on *The Governance of Privacy* (2003: 132-133) and by Abraham Newman in *Protectors of Privacy* (2008: 39-40). For a more sustained analysis of Safe Harbor, see William Long and Marc Pang Quek, "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise", *J. of Euro.Pub. Policy* 9 (2002: 325-344).

[3] Schrems' case against Facebook in Ireland can be found in "Schrems v. Data Protection Commissioner", IEHC 310, bailii.org, High Court of Ireland. Schrems' claims can be found on the website his group created to publicize his case, "Europe versus Facebook", at Europe-v-facebook.org

[4] Ireland is one of the less confrontational European countries with respect to the tech industry, as the recent Apple/European Commission dispute revealed. See the article by James Kantor and Martin Scott, "Apple Owes $14.5 Billion in Back Taxes to Ireland, E.U. Says", *New York Times*, August 30, 2016. http://www.nytimes.com/2016/08/31/technology/apple-tax-eu-ireland-html?_r=0

[5] The proceedings of the CJEU in the Schrems case are summarized in "Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems". EU Law Analysis, March 29, 1915. http://eulawanalysis.blogspot.ie/2015/03/does-facebook-and-usa-violate-eu-data.html.

Second, Europeans have a different concept of privacy than Americans, and different institutional structures to regulate privacy rights.[6] These differences lie at the heart of the "incompatible regimes" in the second part of the title.

Third, the increasing securitization of the Internet and the Snowden affair that exposed it, were a spur for the "contentious challenges" – like Schrem's – in the third part of the title. On both sides of the Atlantic, from the beginning, privacy advocates have attempted to achieve more vigorous protection of personal data, but it was only after the shift from intergovernmental to state-level intrusion on the Internet, that a truly transnational movement began to form in defense of privacy. There is now increasing mutual awareness and cooperation among privacy and consumer NGOs on both sides of the Atlantic.

Not only that: In recent campaigns, firms and non-state actors have been increasingly found on the same side, as in the recent conflict between Apple and the FBI after the San Bernardino terror attacks,[7] adding financial and political heft to the marginal power of NGOs.[8] This has created a much more complex network of interactions than a simple "intergovernmental network" (Raustiala 2002) or even than the "governance triangles" described by Kenneth Abbott and Duncan Snidal (2009).[9] It is part of a complicated transnational network – what Robert Keohane and

---

[6] Of course, privacy is not the only domain where such differences are marked. In his comments on an earlier version of this paper, Michael Dorf reminds me that intellectual property rights, environmental regulation, refugee issues are all treated differently on both sides of the Atlantic. What seems decisive in the case of privacy is a different cultural overlay (see Whitman 2004), the presence of privacy authorities in Europe and their absence in the U.S., and the much greater power of business and the ideology of the market in guiding regulation (see Regan 1995 and 1999 for evidence).

[7] Ellen Nakashima, "Google, Facebook and Other Powerful Tech Firms Filing Briefs to Support Apple". *The Washington Post*, February 28, 2016. www.washingtonpost.com/world/national-security/google-facebook-and-other-powerful-tech-firms-filing-briefs-to-support-apple/2016/02/28/beb05460-de48-11e5-846c-10191d1fc4ec_story.html. For a list of amicus briefs and letters to the court as of March 3, go to http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html.

[8] In much of the literature on digital communications, the large tech companies appear as "villains", influencing state and European policies on privacy, However, as Kristin Eichensehr notes in a personal communication, "we are increasingly seeing companies take privacy protective stances vis-à-vis the government, as for example in the recent Microsoft Ireland case (https://www.justsecurity.org/wp-content/uploads/2016/07/Microsoft-Ireland-2d-Cir-Opinion-20160714.pdf), and attempting to shift the U.S. regime in a more pro-privacy direction."

[9] In their 2009 paper, Abbott and Snidal characterized these groups broadly and assumed that actors in each group pursue their own interests and values when they bargain for influence. Their "triangle" represents actual schemes of transnational agreements and takes in a wide variety of institutional forms, ranging from predominantly domestic state regulation to firm self-regulation, to NGO-initiated schemes, and finally to joint and multi-actor arrangements.

Joseph Nye described as "complex interdependence" (2001 [1979]), and that I have called, in previous work, "complex internationalization".[10]

This paper is an early effort to begin to understand the tangled transnational, transgovernmental, and inter-movement ties among civil society activists, private firms, states, and international authorities in the crucial sector of electronic communications in Europe and the United States. In it, I will ask three questions.

First, can international institutions overcome the disjunction between close interaction and incompatible regimes?

Second, how did the Snowden revelations affect the tangled relations over digital exchange between Europe and the United States?

Third, are these evolving relationships creating the political opportunity for something we can reasonably call "a transnational social movement"? [11]

I will argue that the transnational interactions produced by the digital communication revolution created incentives for non-state actors to intervene in the conflicts among political authorities, but the incompatible privacy regimes of Europe and America impeded common action. It was the growing evidence of state surveillance after 9/11 – and especially after the Snowden revelations - that expanded the political opportunity for mobilizing a transnational movement to defend privacy across the Atlantic. I will begin with some theoretical reflections on the relationship between globalization and complex internationalization before turning to the difficulty of forming a transnational privacy movement, to the changes in the field of privacy since the Snowden revelations of 2013, and finally to the role of civil society actors in challenging public policy.

---

[10] By this term, I intend not merely interdependence among states, but a triangular set of relations among states, international institutions, and non-state actors. Tarrow, *The New Transnational Activism*, (2005).

[11] The concept of "political opportunity structure" comes from the literature on social Movements (see Tarrow 2011, chap. 8, but has been applied by by IR scholar Kathryn Sikkink to transnational mobilization in her "Patterns of Dynamic Multilevel Governance" (2005).

I. INTRODUCTION

During the 1990s, globalization and the information revolution seemed to many scholars and publicists like an inexorable force that was reducing the power and sovereignty of states. This work came on the heels of a generation of research on interdependence, triggered by Robert Keohane's and Joseph Nye's book, *Power and Interdependence*, in the 1970s ([1979] 2001). Some scholars and many publicists saw globalization as a synonym for interdependence, but the two phenomena are analytically separable. As Michael Zürn writes,

> "*The notion of globalization differs from that of interdependence in that it refers to qualitatively different conditions. Whereas the notion of interdependence refers to a growing sensitivity and vulnerability between separate units, globalization refers to the merging of units*" (2002: 235).

This difference is crucial, for while states accept, and even foster interdependence through treaties, contracts, and the formation of intergovernmental networks (Mattli and Woods, eds. 2009), they have naturally resisted "the merging of units". Some important actors – like former President Nicolas Sarkozy of France – think states are still the major actors in governing economic communications. With classical Gallic *suffisance*, Sarkozy told an e-G8 summit that "*Nobody should forget that governments are the only legitimate representatives of the will of the people in our democracies. To forget this is to risk democratic chaos and anarchy*" (quoted in Mansell 2012: 148). On the opposite extreme, some policy makers and advocates argue that the Internet is "ungovernable" because of its global reach. As John Perry Barlow famously put it;

> "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*"[12]

Between these polar positions, many observers have called for consensus-based policies for the internet, devised by diverse groups of government, private sector, and civil society stakeholders. In this spirit, Kal Raustiala sees globalization as producing "transgovernmental regulatory coop-

[12] https://www.eff.org/cyberspace-independence. For the story of how Barlow came to write his provocative paper, go to https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/.

eration", both through classical internationalist mechanisms like treaties and through networks (2002: 14). "Champions of transgovernmentalism," he writes,

> *"(...) agree that the information revolution and globalization are changing world politics and international law. But they believe the state is resilient and will remain the centerpiece of the international system. The state increasingly exercises its power, however, in a disaggregated, flexible fashion that echoes the complexity of the world around it"* (Raustiala 2002: 19).

Where do non-state actors fit in this disaggregated, flexible structure? Kenneth Abbott and Duncan Snidal found that the NGOs in the "governance triangle" were the principal actors in seven of the 39 transnational regulatory schemes they studied and were active participants in 13 others, either jointly with firms or in triangular firm/state/NGO interactions. Indeed, NGOs took the lead in establishing many of these schemes and even stimulated many others (2009: 50; 56).[13] This is what I have called "complex internationalization", in which international institutions serve as a kind of "coral reef" in whose interstices non-state actors can advocate, meet others like themselves from other venues, and form transnational coalitions.[14] As Milton Mueller and his collaborators write, in transnational policy networks "*contentious political actors of all types cluster around authoritative institutions seeking influence*" (Mueller et al. 2007: 269).

But Abbott and Snidal's "governance triangles" operate at the level of *intergovernmental* relations; what happens when there is an upward scale shift from economic issues to national security?[15] Critical junctures like 9/11 turn intergovernmental arrangements into issues of state. This was the case of the Safe Harbor agreement after September 11th, 2001. When word began to leak out that American security agencies were tapping into the internet to troll through millions

---

[13] I have calculated these numbers by eyeballing "the governance triangle" in Figure 2.1 of Abbott's and Snidal's bold effort to plot the relations among states, first, and NGOs. They write that "NGOs have taken the lead in establishing not only Zone 3 schemes [i.e., schemes in which an NGO was the lead actor], but virtually all the collaborative schemes... NGO campaigns also stimulated many firm-and state-based initiatives" (2009: 56).

[14] In a similar vein, Henry Farrell and Abraham Newman write of "the new politics of internationalism, based on their idea that globalization has entered deeply into the fabric of national life" (2014). Jeannett Hoffmann focuses "on those 'critical moments' when routine activities become problematic and need to be revised, thus, when regular coordination itself requires coordination" (Hofmann, et al. 2016: 1).

[15] Keohane and Nye's classical study makes it appear that neat lines divide the field of intergovernmental from interstate relations Their classical contributions are found in their 1972 and 1979 books and in an important 1974 article, "Transgovernmental Relations and International Organizations". *World Politics* 27: 39-62.

of email messages and web browsing, an issue that had been negotiated through the "quiet power" of business-government relations (Culpepper 2011; Rossi 2016:13) became securitized, creating a focal point for privacy advocates on both sides of the Atlantic.

But globalization on its own does not create transnational movements: after two decades of the development of the Internet, in 2001, there was not yet a sustained and unified transnational privacy movement (Bennett 2008). Tech firms like Apple, Facebook, and Google had gained footholds in both Europe and America, and many advocacy groups were active in the general area of privacy but were, for the most part, lodged on one side or another of the Atlantic. When the Snowden revelations burst upon the world, these advocates had not – at least not yet - formed a sustained *transnational social movement*.[16]

Readers who are not *aficionados* of the social movement literature may wonder why it matters whether we call the collection of privacy advocates a "movement" or a "network." It matters, first, because the larger the number of organizations that combine their efforts around transnational issues, the more likely privacy is to be defended. But it also matters because many of the groups that support privacy issues are not *privacy–centered*, but are only *privacy–explicit* or *privacy–marginal* (Bennett 2011). These concentric circles are what have made campaigns for privacy resemble more of a network than a movement.

I define social movements as sustained interactions between organizations and individuals united against common challenges and proposing common solutions to those challenges.[17] Following this definition, I define a transnational movement as *a sustained network of organizations and individuals united across borders against common challenges and proposing common solutions to these challenges.* Although this definition leaves out a great deal of non-state activity for which some would use the term "movement", this more precise definition has the advantage of distin-

---

[16] I define "privacy advocates", with Colin Bennett, as "anybody who might challenge the processing of personal information by government or business". Collier, "Storming the Barricades" (2010: 301). As in most social movements, it is obvious that not all advocates are transnational, and not all those who "challenge the processing of personal information" are advocates. Many are part of institutional groups and others represent political parties.

[17] This definition is drawn from my book, *The New Transnational Activism* (2005). I am aware that there are almost as many definitions of social movements as there are social movement scholars; for a somewhat different, but compatible definition, see Donatella della Porta and Mario Diani, *Social Movements: An Introduction* (2004). What we should *not* do, in my view, is to define every episode of collective action as a "movement".

guishing movements from loose networks of activists who are in contact through the internet or who meet at periodic conferences, and from domestic movements that take foreign or international actors as their targets.

The argument of this paper is that the different privacy regimes in Europe and the United States constituted incompatible opportunity structures that constrained the capacity of privacy advocates to undertake concerted and sustained collective action – at least until recently, when the growing threat of the surveillance of electronic communications has begun to produce greater concertation between privacy advocates on both sides of the Atlantic, as I will show in Part Five.

In Part Two of this paper, I will summarize the major differences between the U.S. and the E.U. privacy regimes. In Part Three, I will examine how international institutions have tried to use their authority in an attempt to resolve this dilemma. In Part Four, I will turn to the difficulties that privacy groups have faced in organizing joint efforts across the Atlantic. In Part Five, I will ask whether recent events have laid the groundwork for the formation of a trans-Atlantic privacy movement.

II. TWO PRIVACY PROTECTION REGIMES[18]

Privacy is an abstract and a much-disputed term. In his landmark study, *Privacy and Freedom,* Alan Westin argued that "*Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists*" (1967: 7). Priscilla Regan divides privacy concerns into three sectors: information privacy, which "involves questions about the use of personal information collected by organizations;" communication privacy –which "involves questions about who can legitimately intercept discussions between two parties"; and psychological privacy issues, which involves "questions about

[18] The following section is based on a reading of work by experts in the privacy field – which I do not claim for myself: Colin Bennett, *The Privacy Advocates* (2008),"Storming the Barricades So We Can All Be Private Together", *Leviathan* (2010), and "Privacy Advocacy from the Inside and the Outside", (2011); Henry Farrell and Abraham Newman, "The Transatlantic Data War", (2016); William J. Long and Marc Pang Quek, "Personal Data Privacy Protection in the Age of Globalization" (2002); Abraham Newman, "Building Transnational Civil Liberties", (2008a) and *The Privacy Protectors* (2008b); Priscilla Regan, *Legislating Privacy* (2008); Regan, Colin Bennett and Robin Bayley, "If these Canadians Lived in the United States, How Would They Protect Their Privacy?" (2016); and Joel Reidenberg, "The Data Surveillance State in the United States and Europe" (2014).

the degree and type of probing utilized in determining individuals' thoughts and attitudes" (1995: 5). The most capacious definition I have found comes from my Cornell colleague, Steven Shiffrin, who writes that "privacy refers to a zone of intimacy in which human beings can live flourishing lives without the intrusion and scrutiny of others" (2016: 13).

When we turn to the differences in how this value is conceived in different parts of the world, we find a fundamental difference. In countries with written constitutions, like the United States, privacy is seen as a civil liberty, with reference to specific national constitutional guarantees, such as the Bill of Rights. But elsewhere, "*claims about privacy as a 'human right' tend to be made in more universalistic terms and derived from certain inherent human rights by virtue of our humanity, rather than our citizenship*" (Bennett 2011: 130). As Abraham Newman notes, the American and the EU systems are extreme cases on a continuum of regulatory systems (2008b: 23).

The simplest way to characterize these two regimes is to say, with Orla Lynskey, that the European model is an "omnibus" regime in which data protection rules are applied to both public and private actors in a sector-neutral way, and are enforced by independent supervisory authorities. In contrast, the American model is a "sectoral", multilevel regime with different legal frameworks applicable to the public and private sector, in which the private sector "is governed by a mixture of ad hoc legislative initiatives, industry self-regulation, and market forces" (Lynskey 2014: 15-17).[19] This created a different opportunity structure for both states and civil society groups in Europe and America. It also created a set of European actors – independent supervisory authorities – who occupy some of the political space that is occupied by civil society groups in America (Bennett 2008: 35).

The EU Data Protection Regime

The most distinctive feature of the European privacy regime is its comprehensive nature and the fact that it is buttressed by a spectrum of national data protection authorities and, since the passage of the Data Protection Directive in 1995, by a European data protection supervisor (Long and Pang Quek 2002). The origins of the European data protection system were national groups of

[19] Note that the 1995 Directive is to be superseded by a new General Data Protection Regulation (GDPR) in 2018. For a brief analysis, see Courtney M. Bowman, "A Primer on the GDPR: What You Need to Know," *Privacy Law Blog*, December 23, 2015, at http://privacylaw.proskauer.com/2015/12/articles-european-union. For a comparison between the 1995 directive and the GDPR, see Lynskey (2014), ch. 2.

privacy activists and lawyers who "formed the core of domestic policy networks involved in developing legislation" (Newman 2008a: 108). "Coming to prominence in the wake of the peace and student movements of the 1960s", writes Newman, "these activists soon turned their attention to the more general societal implications of computer technology" (Ibid.). Out of these efforts grew data protection authorities in a number of EU member states,[20] which were delegated authority to regulate the use of personal information in their countries.

A key turning point came in 1989, when the French national data privacy authority (CNIL), threatened to block data transfers between the corporate offices of FIAT in Italy and France because it held that Italy lacked adequate regulations to guard the privacy of French data (Newman 2008a: 114). A second was the controversy surrounding the creation of the Schengen agreement to permit the mutual policing of national borders, when the French, German and Luxembourg data privacy authorities argued that sharing police information with Belgium – which then had a weak privacy regime – would violate their regulations (Ibid: 115).

As the boundaries of individual European economies eroded with the approach of the single market, these agencies began to work together to play a critical role in promoting data privacy at the European level (Newman 2008b: 11). As Newman writes,

> "*These agencies had a dual motivation: the belief that all Europeans deserved basic privacy protection and a desire to protect their regulatory authority from assault during the creation of the internal market. (…) Fearing that firms would relocate their data processing operations to countries without data privacy rules, regulators in countries such as France and Germany formed transgovernmental networks to lobby for European action*" (Ibid.).

The EU directive that resulted "*forced reforms that strengthened privacy protection and civil liberties within the member states and created a structured system of oversight for the entire region*" (Ibid.).[21] The pre-existing national authorities remained in place to monitor business practices in

[20] The first stage was actually the signature of a Convention of the Council of Europe in 1981, which was signed by Austria, Denmark, France, Germany, Luxembourg, Norway, Spain, Sweden and the United Kingdom. See Neuman (2008a: 109-10) for these efforts.

[21] A good summary can be found in Bennett and Raab, *Governance of Privacy*, (pp. 19,78-80), who also provide a list of the diffusion of data protection legislation in Europe and elsewhere (p. 102), and of the agencies with authority to protect privacy in OECD countries (pp. 108-9). For a sustained analysis of the Data Privacy Directive and of the progress of data protection in Europe before the passage of the GDPR, see Abra-

their countries and consider complaints from citizens who felt their rights had been abused. Their interests and concerns were represented at the European level by what was called the "Article 29 Working Party" – an institutional interest group that draws on national privacy authorities and serves as an advisory body to the Data Protection Supervisor and issues opinions on changes in data protection practices.

The passage of the European Privacy Directive was slow, halting and provided numerous veto points at which regulation-shy European and American business groups could aim their critiques. As Priscilla Regan wrote on the capacity of European and American business to influence the shape of the Privacy Directive; "There are three primary reasons why the European-based strategy was successful: "The timing of the directive, the complexity of the process, and its length provided business associations with the opportunity to organize on both sides of the Atlantic" (Regan 1999: 200). These processes led to ambiguities in the wording of the Directive, to confusion about its implementation, and to conflicts between the strict regime of data protection it threatened, and different regulatory regimes in other parts of the world. But because national data authorities had the leverage to obstruct the free flow of data across national boundaries, they were able to bring about a shift in the scale of data protection from the national to the European level and influence the protection of privacy around the world (Newman 2008b: 116).

The sheer market power of the European economies helped convince Europe's trading partners to adopt European-type data privacy regulations (Newman 2008a). But market power was not limited to Europe. The most persistent conflicts arose between the EU – with its developing regional data protection regime - and the United States, where no such institutions existed and where the lobbying power of private interests heavily outweighed the norm of privacy in debates over privacy (Regan 1995). The market power of American firms and the strength of market-oriented ideology led the United States government to resist acceptance of European norms for the protection of privacy and to agreement on a stopgap measure to allow trans-Atlantic exchange of data to grow – Safe Harbor.

---

ham Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (2008).

The U.S. Data Protection Regime

If the European data protection regime is an "omnibus" one, the American one is sectoral, confusing, and market-oriented. It is sectoral because it is composed of different regimes of privacy protection for different parts of the economy; it is confusing because it is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns; and it is market-oriented because "Americans tend to be more trusting of the private sector and the free market to protect personal privacy – fearing more the invasion of privacy from the state and not the market" (Long and Pang Quek 2002: 331).[22]

Americans were not immune to the need for privacy protection. Priscilla Regan counted 71 congressional hearings between 1965 and 1988 in the field of information privacy and 70 on communications privacy (1995: Appendix A and B).[23] Laws were passed as the result of this legislative activity, but although the Electronic Communications Privacy Act and the Stored Communications Act imposed restraints on the government's access to information,[24] no central institution was created to process claims that privacy was being abused.[25] In the meantime, in the growing realm of the Internet, where private firms frequently retain and market the information of individual users, no legislation was passed to protect citizens' personal data.[26]

---

[22] It might be supposed that federalism and the separation of powers were responsible for the jumble of jurisdictions, laws, and practices that litter the American privacy landscape. But Canada, also a federal system, has a centralized Office of the Privacy Commissioner (OPC) and a national Personal Information Protection and Electronic Documents Act (PIPEDA) which governs the private sector's commercial activities.[22] In an ingenious paired-comparison with the United States, Priscilla Regan, Colin Bennett and Robin Bayley show that this single point of contacts for privacy complaints provides a distinct advantage to the privacy of the average citizen (Regan, Bennett, and Bakeley 2016).

[21.] Milton Mueller and his associates have carried out a thorough analysis of congressional hearings on communications and information privacy in the United States. See their report "Reinventing Media Activism: Public Interest Advocacy in the Making of U.S. Communication-Information Policy, 1960-2002" at http://arifyildirim.com/ilt510/milton.mueller.pdf. An extract from this research, Mueller, et al. (2004), will be examined later in this paper.

[24] 18 U.S.C, &&2510-2522 (2012) and && 2701-2712.

[25] The new Consumer Finance Protection Bureau may eventually grow into that role The CFPB was created by an act of Congress in 2011 in the wake of the financial scandals that had created the Great Recession of 2008. For a brief introduction, go to http://www.consumerfinance.gov/

[26] The most dramatic recent change was the approval by the Federal Trade Commission to prevent companies like AT&T and Comcast from collecting and giving our digital information about individuals – such as the websites they visit and the apps they use. Although the FCC has general responsibility for regulating communications, this was the first time the agency has passed protection of online communications. See Cecilia Kang, "Broadband Providers Will Need Permission to Collect Private Data," *New York Times*, October

Instead, the Office of Management and Budget (OMB) and the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) enforce specific privacy laws, while entire sectors of the economy depend on the "self-regulation" of private actors. "Under this form of private-public regulation, publicly announced corporate policies and industry codes of conduct are backed by the FTC and state-level enforcement in response to private civil actions for damages or injunction relief" (Long and Pang Quek 2002: 333).

There is no simple reason for *why* the American privacy regime became so fragmented, dispersed, and ineffective, but we can trace *how* it happened: it was a classical result of a policy-making process in which abstract principles clashed with the interplay of interests, and in which the most well-placed interests eventually prevailed. Priscilla Regan's narratives of the difficulty of getting effective privacy legislation through Congress, of the unwillingness of the courts to enter this policy area, and of the ultimate dominance of private interests over the ideal of privacy tell a depressing story of lost opportunities, complex and confusing compromises, and the failure to understand the social – rather than the purely individual – nature of privacy (Regan 1995).

It was through the acceptance of a form of "self-regulation" in the implementation of Safe Harbor that the Commission closed its eyes to the absence of a privacy commission in its largest economic partner. This was the internal regime from which the United States resisted adapting its privacy regime to the European Privacy Directive. It managed, instead, to fashion a compromise with the Europeans through a mechanism for government-sanctioned self-regulation by businesses that promised to respect their customers' privacy – the U.S.-EU Safe Harbor agreement (Regan 1995: 1999). But when two airplane-bombs destroyed the World Trade Center on September 11th, 2001, this mechanism – created to monitor commercial digital relations – encountered a "spillover" from commercial exchange to security incentives.[27]

27, 2016 at http://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html?_r=0.

[27] I have sketched several other areas of "spillover" from domestic to national security incentives in a recent book, *War, States, and Contention* (2015) and in a lecture, "Critical Junctures and Institutional Change: How 9/11 is Changing the American State" presented at the Berlin Social Science Center in October 4, 2016, available at https://www.wzb.eu/en/upcoming-events/event-series/distinguished-lectures-in-the-social-sciences.

III. FROM COMMERCIAL EXCHANGE TO THE INTERNATIONAL EMERGENCY

The European Union's 1995 Data Protection Directive was not the first international instrument intended to monitor and control the unregulated diffusion of private data. Two early instruments from the OECD and the Council of Europe "were designed to harmonize data protection policy and force those without appropriate safeguards to pass equivalent legislation" (Bennett and Grant 1999: 12; also see Rotenberg and Jacobs 2013). But because neither instrument-created enforcement mechanisms, either at the intra-state or at the interstate levels, was particularly successful. It was largely in response to these failures and to the growth of global commercial exchanges in the 1990s that the countries of the European Union negotiated a general directive on "the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" between 1990 and 1995 (Ibid.). During the discussions over the Directive, the EU was engaged in absorbing the new post-Communist states of East-Central Europe and had little attention to spare for the intricate technical nuts and bolts of trans-Atlantic data protection or with the interface between commercial exchange and national security.

The Safe Harbor agreement, which followed the passage of the directive by five years, fit within the boundaries of Abbott and Snidal's "governance triangle" of states, businesses, and NGOs – but only just:

First, it was negotiated between an international institution – the European Commission – and a department of a national state – the Department of Commerce. The asymmetrical nature of this exchange gave the agreement an unstable character from the beginning.

Second, the agreement depended for its implementation on the firms that signed up for it, which were responsible for self-monitoring the protection of the data sent to the United States by their opposite numbers in Europe. As such, the agreement had more the character of a contract than an international regulation.[28]

Third, and most important, the discussions were largely couched in political-economic terms (Long and Peng Quek 2002), and did not encompass what would be the biggest thorn in its

[28] As Lingjie Kong writes of such third-party agreements, "Such contracts do not provide a waterproof guarantee; questions remain as to the possibilities of controlling their implementation or enforcing their clauses." (Kong 2010: 448).

side after 2001: the growing interest of America's intelligence agencies in trolling through masses of personal data for evidence of terrorist activity. After September 11th, 2001, and especially with the passage of the U.S. Patriot Act in early 2002,[29] "the United States," as Henry Farrell and Abraham Newman write in a spirited *Foreign Affairs* article, "began to exploit interdependence, by deliberately using its economic power as an instrument of national security" (2016: 125).

We can best understand the vulnerability of the agreement to a national security spillover if we recall the basic distinction, from Keohane and Nye's work, between matters of national security and matters of less importance. In *Power and Interdependence*, Keohane and Nye made three cardinal assumptions:

- *first*, where questions of national security and state sovereignty are concerned, the center of gravity of policy-making gravitates to the highest levels of the executive in relations with the executives of other states;
- *second*, when multiple channels connect societies below the inter-state level, informal ties develop between governmental agencies below the state-to-state level;
- *third*, when there are no clear or consistent hierarchies of military and non-military issues, a plurality of domestic actors is legitimized to participate in world politics. From this process, Keohane and Nye detected a spillover effect, leading to "the proliferation of international activities by apparently domestic agencies" (1979 [2001]: 241).

But "spillover" can be reversed: in times of international crisis, some sectors of activity that lie nominally outside of the security sector can become "securitized." Securitization was especially marked after 2001, as the United States and its allies became preoccupied with the heightened state of alarm over terrorism. In some policy areas – such as identifying airline passengers before their flights took off – European authorities bowed to American demands.[30] In others - such

[29] A brief synopsis of this critical legislation, passed by Congress at the insistence of the Bush administration soon after the September 11th terrorist attacks can be found at https://epic.org/privacy/terrorism/hr3162.html. For the general impact of 9/11 on Americans' privacy see Lyon (2003).

[30] "Agreement Between the European Community and the United States of America on the Processing of the Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, the Bureau of customs and Border Protection". May 24, 2004 at http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf. This early

as freezing the assets of individuals and groups suspected of terrorist ties – European institutions became an adjunct of the UN Security Council's anti-terrorist financing policy and, indirectly, of American policy.[31] Safe Harbor, which began as a political- economic arrangement, was not rewritten in the light of the new security environment, but was eventually undermined by the evidence that came to light of American security agencies' infiltration of private communications between Europe and the United States.

Given the changing balance of commercial exchange and security in European-American relations after 2001, it was likely that the agreement would end up in the courts. That likelihood became virtually inevitable after 2013, when the Snowden revelations made it all but certain that the National Security Agency had been amassing the data of Europeans in its almost obsessive drive to "collect everything".[32] Already in 2013, an Irish NGO – Digital Ireland – had contested the Irish government's data retention law in the CJEU and the court declared the Directive invalid (Lynskey 2014: 163-165). Even before the Schrems decision came down, the Article 29 Working Party "had gone so far as to declare that the implementation of the Data Retention Directive was unlawful" (Reidenberg 2014: 597).

In his CJEU filing, Schrems argued that, "*in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency, the NSA), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country.*"[33]

The Court agreed with Schrems,[34] maintaining that "the United States safe harbour scheme (...)

---

agreement was twice revised, both in 2007 and 2011. For these changes, caused by the Bush administration's willingness to exempt airline passenger information from the Privacy Act, go to https://en.m.wikipedia.org/wiki/United_States%E2%80%93European_Union_Agreement_on_Passenger_Name_Records.

[31] The key *Kadi* cases involved relations between these institutions. For a brief account, see Morse and Keohane (2014).

[32] Former NSA director Keith Alexander was later quoted as saying; "*Yes, I believe it is in the nation's best interest to put all the phone records into a lockbox that we could search.*" http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records.

[33] Court of Justice of the European Union, Press Release No. 117/15. Judgement in Case C-362/14. Maximilian Schrems v Data Protection Commissioner, Luxembourg, October 6, 2015.

[34] The decision will be found at Curia.europa.eu/documents-JSF?number=C-362/14. For a reasonably balanced account, see Natalia Drozdiak and Sam Schechner, "EU Court Says Data-Transfer Pact With U.S. Violates Privacy". *Wall Street Journal*, October 6, 2015. http://www.wsj.com/articles/eu-court-strikes-down-

enables interference, by the United States public authorities, with the fundamental rights of persons." The Court added that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*" and "compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law."[35]

At a stroke, the Court's intervention ended Safe Harbor and led to its successor in 2016, the so-called "Privacy Shield". After intense and arduous negotiations, the text was released in February 2016, remarkably quickly after the CJEU decision, and went into force on August 1st of that year. Secretary of Commerce Penny Pritzger called the agreement "a tremendous victory for privacy for individuals, and businesses on both sides of the Atlantic", one that would "*help grow the digital economy by ensuring that thousands of European and American businesses and millions of individuals can continue to access services online.*" [36] One immediate impact was that the Irish Data Protection Commission filed a new case with the European Court to determine whether Facebook could continue to transfer data from the EU to the U.S. after the invalidation of "Safe Harbor".

Digital Ireland and *Schrems*, alongside the discussions surrounding the passage of the new General Data Protection Regulation, are promising moves for the protection of privacy rights, but neither one will modify member states' own surveillance practices. At the European level, will there be more cases like *Digital Ireland* and *Schrems* brought to the courts by privacy advocates? Will the international situation continue to lead governments to sidestep these agreements in the name of fighting terrorism? Will the persistent conflicts over the protection of privacy between Europe and the United States produce what we can reasonably call a transnational social movement? These are the next two questions that this paper addresses.

---

trans-atlantic-safe-harbor-data-transfer-pact-1444121361. A more technical, but still brief analysis will be found in "European Court of Justice Invalidates US-EU Safe Harbor", October 8, 2015. http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safe-harbor-agreement.

[35] "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid". Court of Justice of the European Union press release No. 117/15, Luxembourg, October 6, 2015, at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[36] The agreement and ancillary documents are at https://www.privacyshield.gov/welcome. Pritzger's laudatory words can be found at https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-release-eu-us-privacy.

IV. CONSTRAINTS ON TRANSNATIONAL MOBILIZATION

Until recently, European and American groups were slow to organize across the Atlantic to contest restrictions on privacy. Even as dedicated an activist as Simon Davies of Privacy International had to admit as much, when he wrote of the international realm that it is there that the privacy movement faces its greatest challenge: "The idea 'Think global, act local' has become a *modus operandi* for the privacy community," he wrote in 1999,

> "*but it is an approach that may ultimately undermine privacy reform. While international business possesses the market power and the global incentive to mobilize against the regulation of data diffusion at the international level, most activists are occupied fighting fires on domestic turf*" (Davies 1999: 259).

The greater cohesion of business associations was revealed when, in 2004, the Executive Coordinator of the UN-sponsored Working Group on Internet Governance invited both business and civil society groups to propose lists of possible candidates for membership in the group. For business, the International Chamber of Commerce contacted over a hundred ICC members and quickly came up with a list of candidates, most of whom became members of the WGIG. "In contrast, when the Executive Coordinator asked for nominations for representatives of civil society, the result was a prolonged and conflict-ridden debate" (Flyverbom 2011: 52-54).

There are three main reasons why it has been difficult for civil society advocates to form a sustained transnational movement—*the intermittency of opportunity to mobilize, differences in the political opportunity structure,* and shift from privacy as a commercial issue to its *securitization.* But as we will see, it was the growth of surveillance in Europe and the United States – and its exposure - that produced the greatest increase in joint mobilization across the Atlantic.

Intermittency

Electronic communication has become so routine and so central to people's lives that it has been difficult for privacy advocates to call attention to its potential for restricting personal freedom, except when well-publicized exposures call the public's attention to these risks. Privacy is "a thousand miles wide and an inch deep", as Colin Bennett quips, noting the "risk that an ideologically thin network is more amenable to temporary campaigns rather than long-term strategic

partnerships" (2008: 193). Rather than building a movement incrementally, the privacy network has gone from episode to episode.

One of the main reasons for the weakness of transnational social movements in general is that the political opportunity structures to which they respond are largely intermittent – like the periodic meetings of the major international financial institutions (Tarrow 2005). When occasions to mobilize are intermittent, so are the efforts to mobilize against them.

Despite their dramatic nature, episodes like the Snowden revelations do not come more than once in a decade, and – in Europe, at least – its memory soon paled before the more immediate crisis of the waves of immigrants attempting to enter Europe from the Middle East and North Africa and the terrorist violence that has broken out in Belgium, France, and Germany. While Snowden's discoveries led to a series of damaging revelations in the United States and to a replacement for the USA Patriot Act,[37] in Europe, fear of renewed terrorist outrages is leading to the prospect of tightened security arrangements and enhanced surveillance.[38]

Political Gaps

As we have seen, the European and the American environments for the regulation of transnational communication are very different—beginning with the terms used on either side of the Atlantic - "privacy" being the preferred term in the United States and "data protection" in the European Union. For some, data protection is a facet of the right to privacy (Lynskey 2016: 101-3), while for others the two terms are distinct, and for still others they overlap. When American and European advocates interact – particularly given language differences – they need to be sure they are talking about the same problem.[39]

---

[37] Public Law No. 114-23 (June 2, 2015, 114th Congress). For a balanced assessment of the strengths and weaknesses of the replacement for the Patriot Act, see Cindy Cohn and Rainey Reitman, "USA Freedom Act Passes: What We Celebrate, What We Mourn and Where do We Go From Here". *Electronic Frontier Foundation,* June 4, 2015. https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here.

[38] For example, in France, in what is already one of Europe's most carefully surveilled societies, there is open discussion of the possibility of interning French citizens suspected of sympathy for terrorism. See Adam Nossiter, "What Price for a Safe France? Perhaps a Country's Core Values, Many Fear," *New York Times*, August 6, 2016. http://www.nytimes.com/2016/08/06/world/europe/france-terrorism-security.html?_r=0.

[39] Legal historian James Whitman (2003-4) focusses on cultural inheritance in explaining the different pri-

The existence of official data protection authorities in Europe and their absence in the United States makes collaboration across the Atlantic difficult. Colin Bennett argues that "[t]he growth of official data protection authorities can have the effect of crowding out the policy space for non-governmental advocacy groups" (2008: 35). For example, in Germany, an early organization, the *Deutsche Vereinigung für Datenschutz*, "declined in importance as the network of German data commissioners (...) became institutionalized" (Ibid.). In the United States, in contrast, the absence of public authorities with responsibilities for privacy has left more policy space for civil society groups to develop.[40]

This difference is reinforced by the greater amount of charitable giving in the United States than in Europe. Groups like the ACLU and the EFF enjoy far more foundation funding than their European counterparts, as well as getting more support from private citizens and corporations. For example, in its 2015 annual report, EFF listed its support from foundations as $998,659, from individuals as $4.7 million, and from individuals donating through foundations at $2.2 million.[41] In contrast, in its 2014-15 financial statement, Privacy International, the London-based international privacy organization, lists total charitable funding as £1,343 million and individual donations as £137 thousand.[42]

But the biggest difference appears to be political, revolving around the greater power of organized business in the United States than in Europe. For example, the first draft of the US Privacy Act had a provision for a privacy protection commission, but was removed after hard lobbying

---

vacy regimes in Europe and the United States. He sees these differences buried in legal history (2002). As Abraham Newman writes, "The European approach toward data protection is grounded in the concept of privacy as a fundamental human right while the U.S. legal system treats privacy as a personal privacy right that may be disposed of as one sees best" (Newman 2008b: 3).

[40] There may also be differences in emphasis between the two clusters of civil society groups. While American groups concentrate on the defense of civil liberties, there is much more diversity in Europe. British-based groups – like the American ones – tend to focus on civil liberties, while continental ones are more oriented to technology, like Chaos Computing in Germany. In addition, much of the work that is carried out by dedicated privacy groups in the U.S. is done by consumer groups in Europe, like the BEUC in Brussels, which divides its activities among a number of consumer-based concerns. I am grateful to Lee Tien of the EFF for these suggestions.

[41] The EFF's 2015 audited financial report can be found at https://www.eff.org/document/fiscal-year-2014-15-audited-financial-statement. Of the corporate foundations, $1.5 million came from a single source, "Humble Bundle".

[42] Privacy International's audited financial report for fiscal 2015 can be found at https://privacyinternational.org/sites/default/files/Audited%20Financial%20Statement%202014-2015.pdf. Note that, unile EFF, Privacy International does not accept corporate contributions.

by business interests.[43] In her exhaustive study of congressional committee hearings on privacy, Regan found that debates that began around the value of personal privacy almost inevitably ended up aimed at other policy priorities and supported those whose interests would be curtailed by privacy protections (1995: 210).

Securitization

Farrell and Newman are certainly correct when they write that, in the early 21st century, the United States has "leveraged the world's reliance on its economy to influence and spy on foreigners" (2016: 125). They join a chorus of critics and analysts who have found in American policies after 9/11 an attempt to create an "international state of emergency" (Scheppele 2004).[44] In the field of financial data protection, the United States government was shown, in 2006, to be using the supposedly secure SWIFT system in Belgium to investigate financial transfers suspected of being linked to terrorist enterprises.[45] More generally, scholars have found a projection of American policy preferences onto international organizations (Kreuder-Sonnen 2016, Tarrow 2015: ch. 8).

Soon after 9/11, the growing perception of the transnational danger of terrorism led American and European security experts to create a High Level Contact Group to lay the groundwork for a more formal EU-U.S. deal on privacy, which "over time tilted the EU's balance away from what they saw as excessive privacy concerns and towards national security" (Farrell and Newman 2014: 11). The final agreement "remade the regulatory bargain over security and privacy within the EU" (2014: 13-14).

---

[43] I am grateful to Colin Bennett for reminding me of this.

[44] I cannot hope to even skim the surface of the vast political science and legal literature on post-9/11 American national security policies. For an excellent survey which emphasizes the growing securitization of international organizations from the European side of the Atlantic, see Christian Krueder-Sonnen,'s PhD thesis, *Emergency Powers of International Organizations,* Free University of Berlin, (2016), ch. 4.

[45] The SWIFT case is briefly summarized by Farrell and Newman (2014: 10). The story of how the USA contravened Belgian privacy laws by breaking into SWIFT bank transfers was broken by the *New York Times* in 2006 and led to a compromise agreement that allowed data transfers to continue. The detailed story in an official Belgian version is found at Commission de la Protection de la Vie Privée, *Opinion on the Transfer of Personal Data by the CSLRT Swift by Virtue of UST* (OFAC), Brussels: Commission de la Protection de la Vie Privée.

But it would be excessive to see this shift in emphasis from rights to security only as the result of the pressure of American policies. Although there was an initial disagreement within the EU after 9/11 between civil rights-oriented officials and security officials, the latter eventually came to dominate negotiations, passing a series of new laws and engaging in practices that seriously compromised the aspirations of the European Charter of Rights. The EU has incrementally tightened the privacy regime that was installed in 1995:

- In 2006, the EU adopted a new Data Retention directive[46] which applied to traffic and location data in order to make it available to law enforcement (Lynskey 2014: 161-3). By requiring service providers to store data and maintain a surveillance database for law enforcement, the directive transforms the private sector into agents of law enforcement. In effect, writes Reidenberg, "Europe has turned online intermediaries into sheriffs" (2014: 601).
- Both the French DGSE and the British GCHQ have been collecting international email traffic of Google and Yahoo and – in the latter case – "capturing all data entering or existing the UK through fiber-optic cables" (Ibid. 2014: 592).
- European intelligence services are afforded privileged rights of access to data. In the UK, France, Sweden and the Netherlands, information can be intercepted without a court order and warrantless wiretapping seems to be much more widespread than in the United States (Ibid: 594).
- There has also been a gradual process of what Colin Bennett and Charles Raab call "function creep". This is the tendency to find new uses and applications for retained data that are unrelated to the purposes for which the data was originally collected (Bennett and Raab 2003: 139; Kreuder-Sonnen 2016: ch. 3; Tarrow 2015: 175-176).

Throughout the process, the objections of both national data protection authorities and of the Article 29 Working Party were largely ignored by the European authorities.[47] Europe has become a "data surveillance state" in the same sense as the United States, according to Joel Reidenberg,

[46] Directive 2006/24/EC, art. 1, 2006 O.J> (L105) 54 EC.

[47] Reidenberg (2014, notes no. 99 and 100) references opinions of the Data Protection authorities and of the Article 29 Working party to the Data Retention Directive that give the flavor of these authorities' vigorous objections.

who feared that "government data surveillance law in Europe and the United States has reached a turning point for the future of information privacy online" (2014: 583).[48]

Will this growing convergence have a positive or negative effect on the potential for the formation of a trans-Atlantic privacy movement? Let us turn to this question now. In December 2015, the European Commission and the European Parliament announced the General Data Protection Regulation, which replaced the 1995 Privacy Directive with binding legislation. While it is true that the new GDPR will leave wide leverage for state security agencies to penetrate privacy – as did the original DPD – it is binding not only on the EU members but on all citizens of the EU, it applies to non-members of the Union, and it offers citizens a mechanism for "the right to be forgotten".[49]

When the GDPR was first proposed in 2012, it was largely seen as a mechanism aimed at ending the fragmentation and costly administrative burdens of the DPD and unifying the widely-varying data protection regimes of the different European states. But in the course of its deliberations, spurred by privacy advocates, by the Article 29 Working Party, and by members of the European Parliament, the Commission added more robust data protection features to the regulation – precisely the opposite of the process that Priscilla Regan had found in the privacy legislation she studied in the American Congress (1995).

What had happened to put steel into a legislative process that more typically leads to the watering-down of legislation? The weakness of Safe Harbor was one possible reason; the geometric growth of trans-Atlantic digital communication was another; but the most important reason was

---

[48] As Orla Lynskey cautions, in actual practice, the European "omnibus" system affords generous exceptions to data regulation for the public sector – especially where national security and police are concerned (2014: 20-23), while the United States may be moving glacially towards the European model (Ibid: 25-26). Lynskey references the emergence of industry self-regulation in areas previously governed by market forces, and what she sees as "an increased impetus for private sector regulation". The Obama administration's proposed "Consumer Privacy Bill of Rights Act" of 2015 was blocked in Congress and was criticized for not going far enough by a coalition of consumer groups. For the White House draft, go to https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf. For an analysis of the bill and its failure to go anywhere, go to http://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html?_r=0.

[49] https://goo.gl/0y49Nphttp://ec.europa.eu/justice/data-protection/reform/index_en. The main legal difference between a directive and a regulation is that while the former allows each government to implement it as their parliaments decide, the latter becomes law in each country in the form in which it is handed down from Brussels.

the explosion of interest in the surveillance of private communication triggered by the revelations by a heretofore unknown contractor for a private firm working in Hawaii for the NSA – Edward Snowden. Much had changed since the beginning of the 1990s, but the Snowden revelations acted as a hinge, bringing together privacy advocates, political actors, and even some of the tech firms who were pushed into a privacy-defending position that their previous behavior would not have predicted.

V. AN EMERGING TRANS-ATLANTIC PRIVACY MOVEMENT?

How much had changed since the early 1990s can be seen from a comparison of conflicts over encryption, over a twenty year period. In 1994, the White House announced that it would make available a cryptographic device, called the "Clipper Chip", which was purported to protect private communications from hacking while allowing the government to obtain the "keys" to the encryption, upon presentation of legal authorization. The underlying algorithm for Clipper Chip, what was known as "Skipjack", had been developed by the NSA. Skipjack was classified as secret on national security grounds, preventing independent evaluation of its capacity to ensure the encryption of private messages.

Sensing the danger of the government's capacity to use Skipjack to infiltrate private communications, a coalition of privacy groups, including the Electronic Privacy Information Center (EPIC) and the EFF, a number of tech firms and cryptographic experts sent an electronic petition – something new at the time – to the government, opposing Clipper Chip. The petition was eventually signed by over 50,000 people, leading the government to eventually back down from the Clipper Chip scheme.[50]

Observe that the entire episode took place within the United States and all of the groups signing the letter denouncing the dangers of Clipper Chip were from within the United States.[51] Now fast forward to January 2016, when a group of 200 activists, digital rights experts, companies and

[50] This summary comes from a somewhat more detailed summary, including the relevant documents at the time, put together by EPIC called "The Clipper Chip", available at https://epic.org/crypto.clipper/default.htm.
[51] The letter will be found at https://epic.org/crypto/clipper/crypto_experts_letter_1_94.html.

organizations called on the Obama administration and other world leaders to oppose any "back doors" to encryption. The petition read, in part,

> *"We urge you to protect the security of your citizens, your economy and your government by supporting the development and use of secure communications tools and technologies, rejecting policies that would prevent or undermine the use of strong encryption, and urging other leaders to do the same."*[52]

The signatories included American stalwarts like the American Civil Liberties Union, EPIC, and the EFF. But more important, the letter was organized by a transnational group, Access Now, which did not exist in 1994, and included signatories from forty different countries. Access Now has organized two "Crypto-Summits", the first in Washington DC in July 2015, and the second in Silicon Valley in March 2016, in conjunction with its annual conference, what it calls "Rights.con," at which the petition was put together and its recipients identified. Table 1 (next page) shows how the debate over encryption and its challenges has become more global and the role of transnational NGOs in the mobilization of a transnational coalition to protect it from state interference.[53]

[52] James Eng, "200 Cyber Activists Urge World Leaders to Reject Encryption 'Back Doors'", NBC News online, January 11, 2016 at http://www.nbcnews.com/tech/security/200-cyber-activists-urge-world-leaders reject-encryption-back-doors-n494191.

[53] The discussion of the group's "Crypto-Summits" can be found on the Access Now Website at www.accessnow.org.

Table 1: Organizations That Signed the "Security For All" letter, by Origin

Geographic location	*Number of organizations*	*Percentage*
Europe	61	33%
North America	56	30%
Asia	25	14%
Central and South America	21	11%
Africa	5	3%
Oceania	4	2%
International*	11	6%
NA**	2	1%
Total	185	100%

Source: "An Open Letter to the Leaders of the World's Governments Signed by Organizations, Companies, and Individuals, January 10, 2016. https://www.securetheinternet.org/

Notes:
* Organizations were coded as "international" when they were either located on more than one continent or were found to have member organizations in more than one country, and a decentralized governance structure.
** Organizations were coded "NA" when no geographic information could be found for them.

Access Now is not the only transnational group that has carried the banner of support for digital rights across borders.[54] For example, in the field of intellectual property rights, in the 1990s, United States policy was essentially written by "rights holders" – big companies that claimed to own the materials they produced. But by 2012, "a transnational coalition of engineers, academics, hackers, technology companies, bloggers, consumers, activists and Internet users defeated the rights holders" (Sell 2013: 67). As Susan Sell concluded: "The ability of Insider/Outsider coalitions comprised of 'rooted cosmopolitans' to shift from lower (...) to higher (for example, bilateral, plurilateral, multilateral, transnational levels and back again for coordinating protest is a powerful political resource" (Ibid: 800).

[54] In a comment on an earlier version of this paper, Agustin Rossi reminds me that the European Green Party and the Pirate Party have played an important role articulating privacy advocacy at the European level. For reasons of space and lack of expertise, I have not investigated either of these party families.

About the same time, in 2011, Colin Bennett – who was originally skeptical of the existence of a transnational privacy movement - has seen the possibility of an integrated privacy network emerging. "The environment," he wrote

> "*now involves a complicated network of private and public sector actors who engage in overlapping domestic and international regimes. (…) Some advocates wish to build a more coherent transnational activist network, which not only uses official means of advocacy and redress, but also engages in a broader 'politics of privacy,' publicly exposing overly intrusive practices and even 'outing' the organizations that are responsible for them*" (Bennett 2011: 126–127).

It was the growing evidence of the extent of the U.S.'s – and, to a lesser extent, the UK's - scooping up of enormous amounts of private digital communication that led to the growing concern with the dangers of state surveillance and with growing evidence of the creation of a sustained transnational movement, and this takes us to "the Snowden effect".

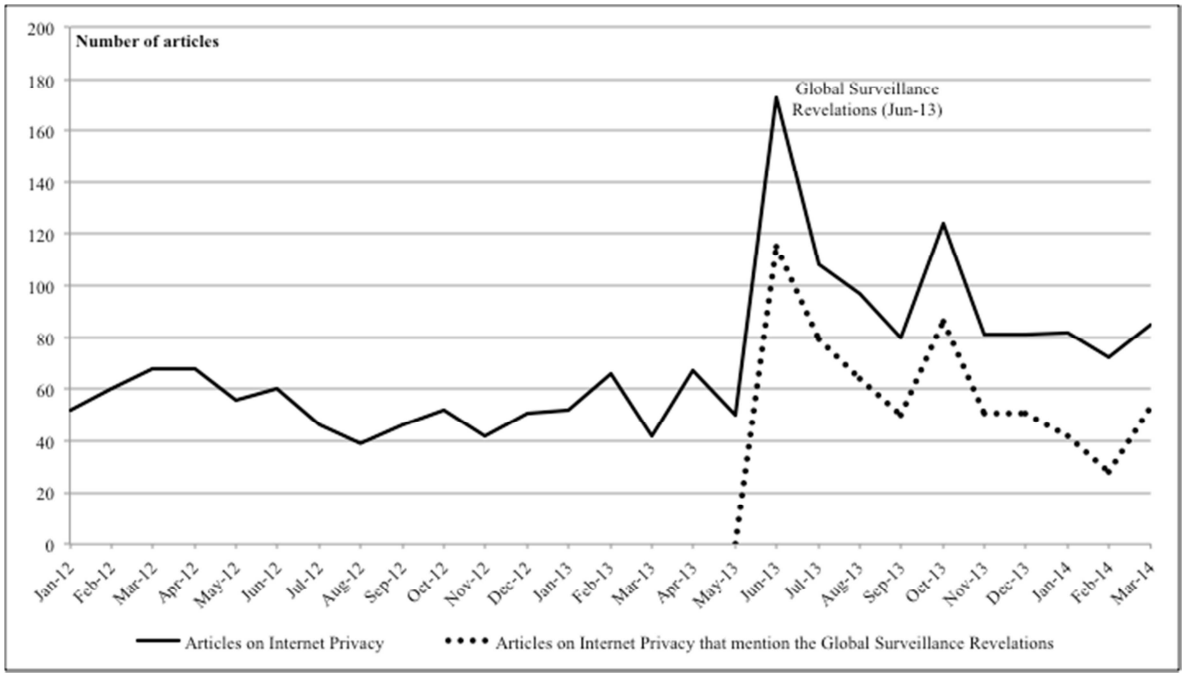
Enter Snowden

Edward Snowden is not a traditional social movement activist; on the contrary, when he decided to reveal his findings, he was a paid contractor of the NSA and had no connection to any social movement organization. He worked with a small group of progressive journalists and publicized his findings through two mainstream newspapers, *The Guardian* and *The Washington Post*. But in the Internet age, the very meaning of social movements has begun to shift, from organizations that use communications media as a mechanism to publicize their claims to small groups of activists for whom communication is their fundamental function (Bennett and Segerberg 2012). Snowden's exploits, using his own digital skills to expose the NSA's secret surveillance programs, may simply be the ultimate extension of this trend.

A young scholar, Agustin Rossi, has so far done the most systematic work demonstrating the increase of interest in surveillance in the mainstream media during and after the Snowden revelations. Using print editions of the main newspapers in the largest EU members – France, Germany, Italy, Spain, and the UK, Rossi carried out a search for news and opinion pieces on Internet privacy or the GDPR from January, 2012 to March 31st, 2014, when the European Parliament voted its position on the Regulation. He found that Snowden's global surveillance revelations tripled the salience of Internet privacy issues and allowed pro-privacy advocates to push

for privacy-strengthening rules in Committee in November 2013 and in Plenary in March 2014. Figure 1 reproduces Rossi's general findings for the five sets of newspaper articles he analyzed.

Figure 1: Salience of Internet Privacy Issues in the Five Biggest EU Countries (January 2013-March 2014)



Source: I am grateful to Agustin Rossi for allowing me to reproduce this graphic from his "Internet Privacy in the European Union and the United States," Unpublished PhD Dissertation, European University Institute, September 2016, p. 42. (Note that there are interesting variations among the five countries' newspapers that he studies, but these do not modify the general trend in Figure One.)

Does this expanded attention to the "politics of privacy" in the European press constitute the objective foundation for a transnational movement? In this preliminary assessment, I can do no more than briefly survey some of the trends that suggest a shift towards a more sustained trans-Atlantic network, including organizational and financial data changes and the growing intersections among European and American organizations with interests in privacy.

More Groups with Greater Funding

In both Europe and the United States, there has been an increase in the funding of existing privacy organizations and a growth in the number and reach of organizations. This growth has been the greatest in the United States, where the threats to privacy have been the most extreme and have been most vividly exposed. For example, the Electronic Frontier Foundation, which report-

ed total income of $4,748 million in 2005-6, had reached an income level of $16,257 million by 2014-15.[55] In the United Kingdom, Privacy International, which reported an income of £487 thousand in 2010-11, had achieved an income level of £1,577 million by 1914-15.[56] Of course, these figures come from among the most prominent privacy groups and may not be representative of the entire sector, but they are indicative of a growing interest in privacy among the public and foundations.

Relatedly, there has been a growth in the number of privacy-defending organizations. Using the systematic source of the *Encyclopedia of Associations* (EoA), Milton Mueller and his associates analyzed public interest organizations whose interests related to the mass media, telecommunications, cable, intellectual property, privacy, and computers from 1969 through 2003 (Mueller et al, 2004: 172). The most rapid growth came in the 1960s and '70s, and was mainly oriented towards "content-oriented activism." By the 1990s, however, the emphasis had shifted to the Internet and was predominantly rights-oriented. These groups included the EEF, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Internet Free Expression alliance, and the Domain Name Rights Coalition. The trend to rights-orientation continued after the turn of the new century, with the appearance of groups such as Public Knowledge, the Center for Digital Democracy, and, more recently, Access Now (Ibid: 179).

Mueller and his collaborators also scanned the LEXIS-NEXIS searchable Congressional Information Service Index for hearings at which communications issues were discussed. Out of a total of 1,771 events that they found in this broad category, the largest number of hearings (N = 227) were primarily about privacy.[57] This does not mean that privacy emerged with greater protection during these decades - on the contrary; Priscilla Regan's work on *Legislating Privacy* found evidence that privacy tended to evaporate in the course of congressional debates (1995); but it does mean that public interest groups interested in privacy were increasingly involved in the political process.

---

[55] These figures come from audited data released by the EFF in 2006 (https://www.eff.org/about/annual-reports-and-financials), and in 2016 (https://www.eff.org/document/fiscal-year-2014-15-audited-financial-statement).

[56] The Privacy International official income figures for these years will be found at https://www.privacyinternational.org/node/102.

[57] Mueller and his collaborators found a much larger number of hearings with "multiple subjects of interest" (N = 429).

Greater Trans-Atlantic Connections

Perhaps more important than either financial or organizational growth, there has been an increase in the number of public interest groups that engage in transnational issues. Already in 2004, Mueller and his collaborators noted "a series of institutional changes with transnational scope, driven by international trade concerns and foreign policy issues" (Ibid: 180). This led to the addition of more international staff and to greater attention to international issues on the part groups like EPIC and the EFF. It has also led to the formation of trans-Atlantic coalitions and campaigns which organize conferences on internet privacy.

For example, in 2015, fourteen U.S. based civil liberties and privacy groups joined twenty European-based groups in sending a joint letter to the EU Commissioner for Justice, Consumers, and Gender Rights and to Secretary of Commerce Penny Pritzker, urging a comprehensive modernization of privacy and data protection laws on both sides of the Atlantic.[58] American civil liberties groups are also beginning to act as *amici* in court cases in Europe alongside their European counterparts, but these observations are too fragmentary to be seen as a trend.[59]

Most important has been the creation and expansion of *Access Now*, which maintains eleven offices around the world, organizes the international Rights.con conference, and has dedicated activities in privacy, digital security, human rights, freedom of expression and net discrimination.[60] Scanning the *Access Now* blog in August, 2016, ten of twelve postings were either international in general, or dealt with a part of the world outside the U.S.[61] Policy-oriented groups are also active participants in academic conferences on privacy, both in the U.S. and in the European Union.[62]

---

[58] See "EU-US Letter on Safe Harbor After Schrems".
http://r.search.yahoo.com/_ylt=A0LEV76NfopXL2cAgo0PxQt.;_ylu=X3oDMTByOHZyb21tBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNzcg--/RV=2/RE=1468722957/RO=10/RU=http%3a%2f%2fthepublicvoice.org%2fEU-US-NGO-letter-Safe-Harbor-11-15.pdf/RK=0/RS=FT_WgXqM4LBMBUmfA7iwmB79D2g-.

[59] For example, in 2016, the Irish High Court accepted EPIC's application to participate in a new case about data protection rights regarding Facebook's contractual clauses. The case follows the CJEU decision to strike down Safe Harbor in 2015. EPIC also recently joined a case before the European Court of Human concerning the activities of British and U.S. intelligence organizations.

[60] https://www.accessnow.org/issue/privacy/.

[61] https://www.accessnow.org/issue/privacy/.

[62] I am grateful to Priscilla Regan for pointing this out to me.

Greater Mutual Attention

To the degree that an international state of emergency has expanded across the Atlantic, European and American privacy groups are increasingly facing a similar structure of opportunity and threat. We can hypothesize that such a common focal point should lead first, to greater awareness of each grouping's concerns on the part of the other, and, secondly, may lead to the eventual formulation of common identities and strategies.

To probe the first hypotheses, with a collaborator,[63] I have collected data on the attention given to privacy issues on the other side of the Atlantic from two of the main non-state actors in the privacy world: EPIC, the U.S. based Electronic Privacy and Information Center, and EDRI, the Brussels-based *European Digital Rights* group. The object of the exercise was to understand whether there has been a reciprocal growth of attention of American-based and the EU-based groups to one another over time. We were also interested in the connections – if any - between "real-world events" – like the Snowden revelations in 2013 and the dispute over Safe Harbor in 2015 – and the growth of mutual attention of European and American privacy groups to one another and to one another's concerns.

In the United States we coded fifteen years of *Epic Alert*, the bi-weekly online newsletter of EPIC, from 2000 through 2015. *Epic Alert* contains articles on privacy developments in the U.S. and around the world, reports on breaking privacy news, reviews of the latest privacy-related publications, and lists upcoming privacy conferences and events.[64] In Europe, we coded every issue of *Edri–Gram*, the fortnightly online newsletter of the Brussels-based group *European Digital Rights*, which covers similar topics to its American-based counterpart for the period 2011-2015.[65]

As Figure 2 shows, the amount of coverage of non-US events or issues in the Washington-based *Epic–Alert* newsletter grew steadily, but moderately, during the first decade of the new century, but increased dramatically after 2012 – when Edward Snowden's revelations appeared - and especially during the debate over the transfer of European data to the United States. A detailed

---

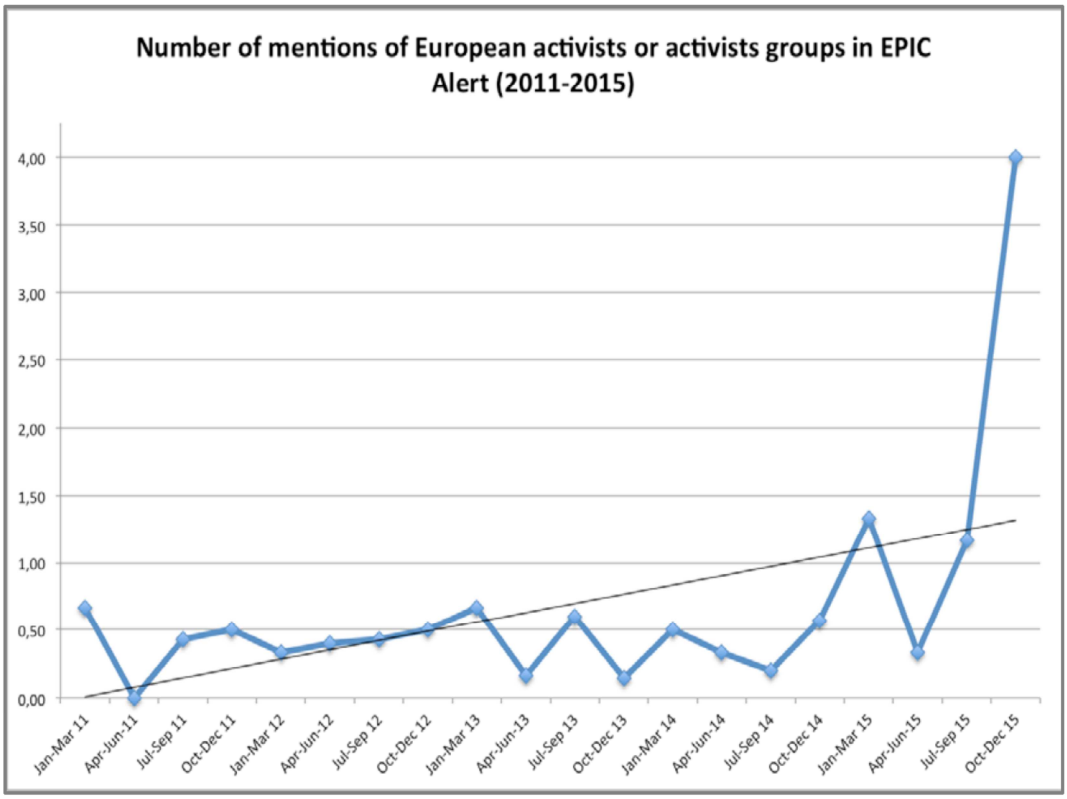
[63] My thanks to Emilio Lehoucq, of the University of the Andes in Bogota, Colombia, for carrying out the coding of these newsletters for this paper.

[64] https://epic.org/alert/.

[65] https://edri.org/newsletters/.

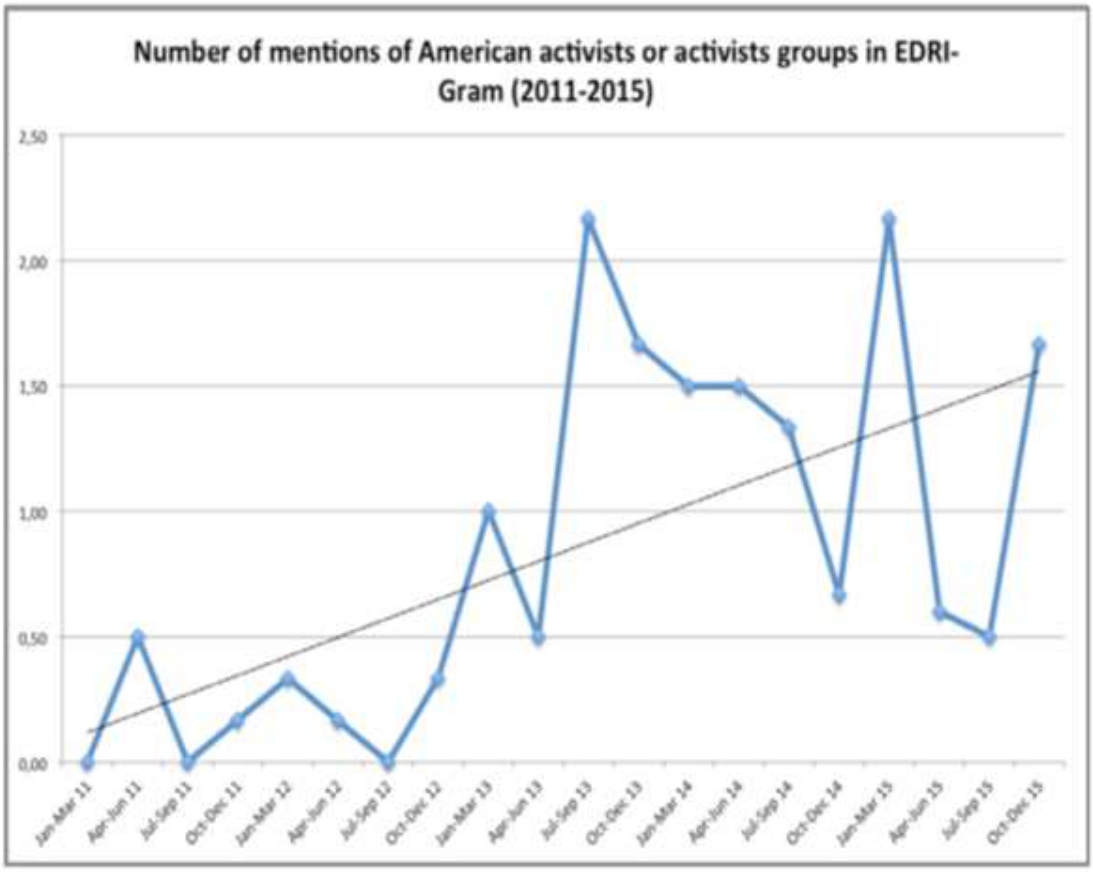
analysis of the issues covered remains to be carried out, but a rapid inspection showed that it was the debate over Safe Harbor and the Privacy Shield that increased EPIC's attention to European developments.

Figure 2: Number of Articles in Epic-Alert Dealing with European Issues, 2000-2015



As Figure 3 shows EDRI's attention to the U.S. also grew over the last half-decade, but did not follow the same trend line as the American data. There has been an increase in attention to American issues in this Brussels-based newsletter since 2011, but the biggest period of growth came in 2013, after the Snowden revelations were publicized in the European press. Of course, although the Snowden case took place in the United States, its reach was truly global.

Figure 3: Number of Articles in EDRi-Gram Dealing with American Issues, 2011-2015



In summary, from an intermittently-mobilized group of primarily and privacy-oriented groups and a spectrum of other groups with privacy as one of their concerns (Bennett 2008), primarily interested in their own countries, we are seeing the formation of a more sustained coalition of privacy advocates, mobilizing around issues like surveillance and encryption and learning to use the courts and public opinion to advance their claims.

CONCLUSIONS

While these findings are too fragmentary to allow me to allow for firm conclusions about the potential growth of a trans-Atlantic privacy movement, there is growing evidence that such a movement is in the process of formation.

Part One summarized arguments from the IR literature about transnational regulatory arrangements. The international scene has seen a growing trend to the formation of transgovernmental

networks, a development that I interpreted as a trend towards what I call "complex internationalization." Using different language, Abbott and Snidal see this trend producing a "governance triangle", which extends from states and private businesses to NGOs. They are largely correct, but their work elides what happens when close interaction clashes with incompatible regimes.

In Part Two, I examined the mix of opportunities and constraints in the EU and the United States in the field of privacy protection. Drawing on research by others, I argued that the European regime – despite its shift towards greater surveillance – is becoming more unified, while the American regime is fragmentary, sectoral, and has been mainly shaped by the interests of industry. Some scholars, like Rustiala, see transgovernmental networks as mechanisms to increase cooperation – or at least, to limit conflict between states. But I argue instead that close interaction plus incompatible regimes produce unstable agreements and the potential for conflict. We saw this in the attempt to bridge the gap between the U.S. and the EU privacy regimes with the Safe Harbor agreement;. We will have to see whether its successor agreement – Privacy Shield – does any better.

In Part Three, I diagnosed the major reason for the failure of Safe Harbor to be a result of the disjunction between commercial concerns, which dominated the negotiation of the agreement, and the security concerns that ultimately unhinged it. Although both the EU and the European Court weighed in on attempting to resolve the issues involved, neither overcame the gap between states' interest in security and the sectoral goal of privacy.

As I argued in Part Four, the intermittent nature of trans-Atlantic opportunities for mobilization, the political differences between the two regions, and the securitization of nominally non-security interactions are obstacles to the transformation of these opportunities into sustained movements. Safe Harbor was ultimately defeated by a privacy advocate taking a government and a private firm to court, which extends the traditional meaning of the term "social movement."

Part Five addressed the question of whether the emerging transnational concern with privacy is laying the groundwork for a trans-Atlantic privacy movement. Data on the growth of funding and organizations aimed at protecting privacy, as well as growing mutual awareness on the part of non-profit groups on both sides of the Atlantic, both suggest a network that may be coalescing

into such a movement.[66] As Regan writes of privacy legislation in the United States, "Privacy advocates were most successful in achieving privacy legislation when they reached beyond the privacy policy communities to form advocacy coalitions with other groups" (1995: 210). Building such coalitions means going beyond intermittent opportunities, overcoming political and institutional gaps, and building an "abeyance structure" (Rupp and Taylor 1987) that will – when a particular battle is over – live on to fight another day. It means building a social movement, which is the only way the power of powerful states can be successfully contested (Cole 2015; Tarrow 2015).

[66] For a stimulating comparison of networks and movements, see Mario Diani and Ivano Bison, "Organizations, Coalitions, and Movements", (2004).

REFERENCES

Abbott, Kenneth W., and Duncan Snidal. 2009. "The Governance Triangle: Regulatory Standards, Institutions and the Shadow of the State". In *the Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods, pp. 44-88. Princeton: Princeton University Press.

Bennett, Colin J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

—. 2010. "Storming the Barricades So We Can All Be Private Together: Everyday Surveillance and the Politics of Privacy Advocacy". *Leviathan* 25: 299-320.

—. 2011. "Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies". *Journal of Comparative Policy Analysis: Research and Practice* 13: 125-41.

Bennett, Colin J., and Rebecca Grant, eds. 1999. *Visions of Privacy: Policy Choices for the Digital Age* Toronto and London: University of Toronto Press.

Bennett, Colin J., and Charles Raab, eds. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgrate.

Bennett, W. Lance, and Alexandra Segerberg. 2013. *The Logic of Connective Action*. New York: Cambridge University Press.

Culpepper, Pepper. 2011. *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. New York: Cambridge University Press.

Davies, Simon. 1999. "Spanners in the Works: How the Privacy Movement is Adapting to the Challenge of Big Brother". In *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin J. Bennett and Rebecca Grant, pp. 244-62. Toronto and London: University of Toronto Press.

Della Porta, Donatella, and Mario Diani. 2006. *Social Movements: An Introduction, 2nd edition.* Malden MA and Oxford: Blackwell's.

Diani, Mario, and Ivano Bison. 2004. "Organizations, Coalitions, and Movements". *Theory and Society* 33: 281-309.

Farrell, Henry, and Abraham Newman. 2016. "The Transatlantic Data War: Europe Fights Back Against the NSA". *Foreign Affairs* 95: 124-133.

Farrell, Henry, and Abraham L. Newman. 2014. "The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes". *Comparative Political Studies* 48: 497-526.

Flyverbom, Mikkel. 2011. *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham, UK and Northhampton MA, USA: Edward Elgar.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance". *New Media and Society* 18: 1-18.

Keohane, Robert, and Joseph Nye. 1972. "Transnational Relations and World Politics: An Introduction". *International Organization* 25 (3).

Keohane, Robert O., and Joseph S. Nye. 1974. "Transgovernmental Relations and International Organizations". *World Politics* 27 (1): 39-62.

— (Eds.). 2001 [1979]. *Power and Interdependence: World Politics in Transition*. New York: Addison-Wesley Pub. Co.

Kreuder-Sonnen, Christian. 2016. "Emergency Powers of International Organizations". In *Political Science*: Free University of Berlin.

Long, William, and Marc Pang Quek. 2002. "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise". *Journal of European Public Policy*.

Lynskey, Orla. 2014. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

Lyon, David. 2003. *Surveillance After September 11*. Cambridge: Polity.

Mansell, Robin. 2012. *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Mueller, Milton, Brenden Kuerbis, and Chrsitane Page. 2007. "Democratizing Global Communication? Global Civil Society and the Campaign for Communication Rights in the Information Society". *International Journal of Communication* 1: 267-96.

Mueller, Milton, Christiane Page, and Brenden Kuerbis. 2004a. "Civil Society and the Shaping of Communication-Information Policy: Four Decades of Advocacy". *The Information Society* 20: 1-17.

Newman, Abraham L. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca and London: Cornell University Press.

—. 2008a. "'Building Transnational Civil Liberties' Transgovernmental Entrepreneurs and the European Data Privacy Directive". *International Organization* 62: 103-30.

Regan, Priscilla. 1995. *Legislating Privacy*. Chapel Hill and London: University of North Carolina Press.

—. 1999. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics". In *Visions of Privacy: Policy Choices for the Digital Age*, edited by Collin J. Bennett and Rebecca Grant, pp. 199-216. Toronto and London: University of Toronto Press.

Regan, Priscilla M., Colin J. Bennet, and Robin M. Baykley. 2016. "If These Canadians Lived in the United States, How Would They Protect Their Privacy?". in *2016 Privacy Law Scholars Conference*. George Washington University.

Reidenberg, Joel R. 2014. "The Data Surveillance State in the United States and Europe". *Wake Forest Law Review* 49: 583-608.

Rossi, Agustin. 2016. "Internet Privacy in the European Union and the United States". in *Political and Social Sciences*: European University Institute.

Rotenberg, Marc, and David Jacobs. 2013. "Updating the Law of Information Privacy: The New Framework of the European Union". *Harvard Journal of Law and Public Policy* 36: 607-252.

Scheppele, Kim Lane. 2004. "Law in a Time of Emergency: States and the Temptations of 9/11". *Journal of Constituitonal Law* 6: 1-75.

Sell, Susan. 2013. "Revenge of the 'Nerds': Collective Action Against Intellectual Property Maximalism in the Global Information Age". *International Studies Review* 15: 67-85.

Shiffrin, Steven H. 2016. *What's Wrong with the First Amendment?* New York: Cambridge University Press.

Sikkink, Kathryn. 2005. "Patterns of Dynamic Multilevel Governance and the Insider—Outside Coalition". In *Transnational Protest and Global Activism*, edited by Donatella Della Porta and Sidney Tarrow, pp. 151-73. New York: Rowman and Littlefield.

Slaughter, Anne-Marie. 2004. *A New World Order*. Princeton: Princeton University Press.

Tarrow, Sidney. 2005. *The New Transnational Activism*. Cambridge and New York: Cambridge University Press.

—. 2011. *Power in Movement: Social Movements and Contentious Politics, 3rd. ed.* Cambridge: Cambridge University Press.

---. 2015. *War, States and Contention.* Ithaca and London: Cornell University Press.

Westin, Alan. 1967. *Privacy and Freeedom*. New York: Athaneum.

Whitman, James Q. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty". *Yale Law Journal* 113: 1151-1221.

Zürn, Michael. 2002. "From Interdependence to Globalization". In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse, and Beth Simmons. London: Sage.

Discussion Paper of the Research Area International Politics and Law
Research Unit: **Global Governance**

Jens Steffek SP IV2014–101
The Democratic Output Legitimacy of International Organizations

Pieter de Wilde, Ruud Koopmans and Michael Zürn SP IV2014–102
The Political Sociology of Cosmopolitanism and Communitarianism:
Representative Claims Analysis

Louis W. Pauly SP IV2014–103
Governing Global Risks:
The Evolution of Policy Capacity in the Financial Sector

Jeffrey T. Checkel SP IV2014–104
Mechanisms, Process and the Study of International Institutions

Xinyuan Dai SP IV2014–105
The Conditional Effects of International Human Rights Institutions

Gary Goertz and Kathy Powers SP IV2014–106
Regional Governance: The Evolution of a New Institutional Form

Matthew Stephen and Michael Zürn SP IV2014–107
Contested World Orders:
Rising Powers, Non-State Actors, and the Politics of Authority
Beyond the Nation-state

John M. Owen SP IV2016–108
Global Power Shifts and the Future of Democracy:
An Evolutionary Approach, with Special Attention to China

Christian Joerges and Christian Kreuder-Sonnen SP IV2016–109
Europe and European Studies in Crisis:
Inter-Disciplinary and Intra-Disciplinary Schisms in Legal and
Political Science

Wolfgang Hein SP IV2016–110
Intellectual Property Rights and Health:
The Constraints of WHO Authority and the Rise of Global Health
Governance as an Element of Contestation

Wolfgang Wagner, A. Herranz-Surrallés, J. Kaarbo and F.Ostermann SP IV2017–111
Politicization, Party Politics and Military Missions
Deployment Votes in France, Germany, Spain, and the United Kingdom